UNITED STATES DISTRICT COURT

for the

District of Utah

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

WESTERN DIGITAL HARD DRIVE BEARING SERIAL NUMBER WMC650D1K71Z

Case No. 4:25-mj-00048 PK

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of Utah, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252A	Transportation/Receipt/Distribution/Possession of Child Pornography
18 U.S.C. 1466A	Possession of obscenity

The application is based on these facts:

See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

IVAN J MURRAY
Digitally signed by IVAN J MURRAY
Date: 2025.05.14 14:17:10 -06'00'

Applicant's signature

HSI SA Ivan Murray

Printed name and title

Sworn to before me and signed in my presence.

Date: May 14, 2025

Judge's signature

City and state: Salt Lake City, Utah

United States Magistrate Judge Paul Kohler

Printed name and title

FELICE JOHN VITI, Acting United States Attorney (#7007)
CHRISTOPHER BURTON, Assistant United States Attorney (NV #12940)
Attorneys for the United States of America
Office of the United States Attorney
20 North Main Street, Suite 208
St. George, Utah 84770
Telephone: (435) 634-4270
Christopher.Burton4@usdoj.gov

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A WARRANT AUTHORIZING THE SEARCH OF A WESTERN DIGITAL HARD DRIVE BEARING SERIAL NUMBER 19528A800170	AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT **Under Seal** Case No. 4:25-mj-00047 PK
IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A WARRANT AUTHORIZING THE SEARCH OF A WESTERN DIGITAL HARD DRIVE BEARING SERIAL NUMBER WMC650D1K71Z	AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT **Under Seal** Case No. 4:25-mj-00048 PK

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, Ivan Murray, Special Agent with Homeland Security Investigations, being duly sworn, state:

AFFIANT BACKGROUND AND QUALIFICATIONS

1. I am a Special Agent with Homeland Security Investigations and have been since November of 2011. I am currently assigned to assist the Federal Bureau of Investigation's Child Exploitation Task Force (CETF) as well as the Utah Attorney General's Internet Crimes Against Children Task Force (ICAC). Prior to my current position with HSI, I was employed as a Criminal Investigator/Special Agent with Internal Revenue Service - Criminal Investigative Division for approximately seven years. I've received training in child-pornography investigations, and I've had the chance to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received additional training from CETF and ICAC relating to online, undercover chatting investigations, as well as peer-2-peer or P2P investigations. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. Specifically, I have participated in numerous investigations relating to the sexual exploitation of children over the Internet since 2013.

PURPOSE OF AFFIDAVIT

2. I submit this Affidavit in support of an application for a search warrant for a Western Digital Hard Drive bearing serial 19528A800170 and a Western Digital Hard Drive bearing serail WMC650D1K71Z (the "Subject Devices"), that are currently secured in the evidence room at the Department of Homeland Security Investigations in Salt Lake City, Utah, at 2975 Decker Lake Drive West Valley City, UT 84119.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts in this affidavit are included based on my training and experience, as well as my review of reports written by other law enforcement officers.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. § 2252A(a)(5) (Possession of child pornography); 18 U.S.C. § 2252A(a)(1) (Transportation of child pornography); 18 U.S.C. § 2252A(a)(2), (Distribution/Receipt of child pornography), and 18 U.S.C. § 1466A (Possession of obscenity) have been committed by JOHNSTON BLACKHORSE (the "Target Offenses"). There is also probable cause to search the Subject Device described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of the Target Offenses as further described in Attachment B.

SEARCH METHODOLOGY TO BE EMPLOYED

5. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as

set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. using hash values to narrow the scope of what may be found. Hash values are used to find previously identified files of images of child pornography and do not capture images that are the result of new production, images embedded in an alternative file format, or images altered, for instance, by a single pixel. Thus, hash value results are under-inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BACKGROUND REGARDING DIGITAL DEVICES

6. Based upon my training, my experience, and my discussions with other law enforcement agents, I know the following:

a. Users of digital devices increasingly choose to store items in digital form (e.g. pictures, documents) because digital data takes up less physical space, and can be easily organized and searched. Users also choose to store data in their digital devices, such as cell phones, because it is more convenient for them to access data in devices they own, rather than to later spend time searching for it. Keeping things in digital form can be safer because data can be easily copied and stored off site as a failsafe.

b. Users also increasingly store things in digital form because storage continues to become less expensive. Today, 500 gigabyte (GB) hard drives are not uncommon in computers. As a rule of thumb, users with 1 gigabyte of storage space can store the equivalent of 500,000 double spaced pages of text. Thus, each computer can easily contain the equivalent of 250 million pages, that, if printed out, would fill three 35' x 35' x 10' rooms. Similarly, a 500 GB drive could contain 450 full run movies, or 450,000 songs, or two million images. With digital devices, users can store data for years at little or no cost.

c. Storing data in digital form and not deleting it mirrors users' online habits where users have, for years, been encouraged to never delete their E mails. For example, on March 27, 2007, Yahoo! Mail announced free, "unlimited" capacity that gave their users "the freedom to never worry about deleting old messages again." See < http://ycorpblog.com/2007/03/27/yahoo mail goes to infinity and beyond/> (accessed April 18, 2012). Similarly, since June 2007, Google, Inc. has promoted free, increasingly larger storage "so you should never have to delete mail." <http://gmailblog.blogspot.com/#!/2007/06/welcome to official gmail blog.html>; see

also <http://gmailblog.blogspot.com/2007/10/more gmail storage coming for all.html> (accessed April 18, 2012) (promoting its "Infinity+1" plan to constantly give subscribers more storage). Hotmail also has advertised free, “virtually unlimited space,” noting that “Hotmail gives you all the space you need.” See <http://www.microsoft.com/windows/windowslive/anotherlookathotmail/storage/> (accessed April 18, 2012).

d. Digital devices can also store data automatically, without a user’s input. For example, network logs may track an employee's actions for company auditing purposes or E mail headers may automatically list the servers which transmitted the E mail. Similarly, a web browser (i.e. an application such as Internet Explorer used to access web pages) can track a user’s history of websites visited so users can more easily re access those sites. Browsers also often temporarily cache files from recently accessed web pages to improve the user's experience by reducing that page’s loading time. These examples illustrate how the interaction between software and operating systems often results in data being stored without a user's knowledge. Even if a sophisticated user understands this automatic storage of data, attempts at deleting this data often fail because the data may be automatically stored multiple times and in different locations. Thus, digital evidence may exist despite attempts at deleting it.

e. Digital data is particularly resilient to deletion. First, as noted, data is often automatically stored multiple times in multiple places, where even sophisticated users may not be able to locate. Second, digital data can be recovered years after it has been saved, or viewed B even after such data has been deleted. For example, when a user

deletes a file on a computer, the file is sent to the recycle bin, where it can still be retrieved. Even if the file is deleted from the recycle bin, the data does not actually disappear; rather, it remains in "free space" or "slack space" (i.e. in unused space) until it is overwritten by new data. Third, an operating system may also keep deleted data in a "recovery" or "swap" file. Fourth, files from websites are automatically retained in a temporary cache, which are only overwritten as they are replaced with more recently viewed web pages. Thus, the ability to retrieve residues of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer use habits.

DETAILS OF THE INVESTIGATION

7. On February 6, 2025, United States Probation Officers Frank Davis and Cordell Wilson conducted a home visit at the residence of Johnston BLACKHORSE. BLACKHORSE is currently on a lifetime term of supervised release as a result of a 2015 conviction for Possession of Child Pornography out of the District of Nevada (Case No. 2:14-cr-00340-APG-PAL). In 2017, a petition was filed alleging BLACKHORSE violated the terms of his supervised release by drawing and selling obscene images depicting the sexual abuse of children. BLACKHORSE's supervised release was revoked and he was ordered to serve six months custody, with a lifetime term of supervised release to follow.

8. Although the February 6 home visit itself was unannounced, BLACKHORSE was enrolled in the Tribal Community Reentry Court (TCRC) program and probation visits often coincide with TCRC court hearings.

9. During the course of the home visit on February 6, BLACKHORSE's computer was reviewed. Probation officers saw evidence of the recent download of a forensic wiping program, CCleaner, on BLACKHORSE's computer. It appeared CCleaner had been installed on the computer the day of the visit, just a few hours before the home visit. When BLACKHORSE was asked about the downloaded software, he denied any knowledge of it. BLACKHORSE confirmed no one else had access to his computer.

10. Probation officers took both hard drives installed in the computer, a Western Digital Hard Drive bearing serial 19528A800170 and a Western Digital Hard Drive bearing serial WMC650D1K71Z (the "Subject Devices"), for further forensic examination. The immediate area was searched for USB drives and external hard drives; none were found. The Subject Devices were then submitted to the Probation Department's forensic lab for forensic review.

11. The Subject Devices were subsequently forensically reviewed at the Probation department forensic lab. Both Subject Devices were successfully imaged. There was significant evidence showing BLACKHORSE was the user of the Subject Devices. This included various profile names for social media accounts bearing BLACKHORSE's name as well as a selfie-style photograph depicting BLACKHORSE holding his driver's license.

12. On the Subject Devices, the forensic examiner found approximately five images of child pornography in deleted space. I received descriptions of those files from Probation and two are included below:

Item ID: 1621931
Filename: unnamed (Carved)
Description: Color photograph of a prepubescent white female child, approximately 8-10 years old, with long blond hair. The female child is lying back on what appears to be a bed with legs spread apart, fully nude with chest and vagina exposed. Female child appears to be lying next to what appears to be a naked adult male with the male's hand around the back of the child. The face of the adult male is cut off the side of the photograph.

Item ID: 1622466
Filename: unnamed (Carved)
Description: Color photograph of a prepubescent white female child, approximately 8-10 years old, with long dark hair past her shoulders. The child appears to be laying fully naked on a large pillow placed on the floor. The child has her legs spread, fully exposing her vagina, with her naked chest also visible.

Additionally, in deleted space, the forensic examiner found additional images of prepubescent girls in various sexually suggestive poses with clothing on and multiple animation of drawn images depicting child sexual abuse. The fact that images were found in deleted space means that they existed on the Subject Devices at some point in time and were deleted by a user. The location of the files in deleted space was consistent with the use of a forensic cleaning program like CCleaner.

13. The forensic examiner also reviewed the internet browser information on the Subject Devices. On one browser, DuckDuckGo, the website history reflected visits to cam4.com and chaturbate.com. There was also evidence of a search for "Youngtube" on the Subject Devices in December 2024.

14. There was evidence of an external drive connection, identified as "(G:)", which contained a folder titled "mmd stuff" that was accessed frequently. There was also

evidence that a USB drive was connected to the Subject Devices as recently as January 1, 2025. As noted above, no external hard drives or USB drives were found during the home visit.

15. The forensic exam also revealed evidence of the CCleaner program, with data suggesting that the program had been accessed on multiple dates in 2024 and 2025.

16. The Subject Devices remain in the custody of the Department of Homeland Security at their Salt Lake City Office, located at 2975 Decker Lake Drive West Valley City, UT 84119.

CONCLUSION

17. Based on the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that the Subject Device contains evidence of Title 18 U.S.C. § 2252A(a)(5) (Possession of child pornography); 18 U.S.C. § 2252A(a)(1) (Transportation of child pornography); 18 U.S.C. § 2252A(a)(2) (Distribution/Receipt of child pornography); and 18 U.S.C. § 1466A (Possession of obscenity) and that the information sought herein will materially aid the investigation.

RESPECTFULLY SUBMITTED this __th day of May, 2025.

IVAN J MURRAY

Digitally signed by IVAN J MURRAY
Date: 2025.05.14 14:14:56 -06'00'

Ivan Murray, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me this 14th day of May, 2025.

JUDGE PAUL KOHLER
United States Magistrate Judge

ATTACHMENT "A-1"
Property to Be Searched

The Subject Device is described as a Western Digital Hard Drive bearing serial 19528A800170, that is currently secured at the evidence room located at the Department of Homeland Security Investigations located in Salt Lake City, Utah, located at 2975 Decker Lake Drive West Valley City, UT 84119.

ATTACHMENT "A-2"
Property to Be Searched

The Subject Device is described as a Western Digital Hard Drive bearing serial WMC650D1K71Z, that is currently secured at the Department of Homeland Security Investigations located in Salt Lake City, Utah, located at 2975 Decker Lake Drive West Valley City, UT 84119..

ATTACHMENT B
LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

This affidavit is in support of application for a warrant to search a Western Digital Hard Drive bearing serial 19528A800170 and a Western Digital Hard Drive bearing serial WMC650D1K71Z, that are more specifically identified in the body of the application and in Attachment A ("Subject Devices"), and can be used to store information and/or connect to the Internet, or which may contain mobile devices, for records and materials that are fruits, evidence, or instrumentalities of violations of 18 U.S.C. § 2252A(a)(5), 18 U.S.C. § 2252A(a)(1); 18 U.S.C. § 2252A(a)(2); and 18 U.S.C. § 1466A (the "Target Offenses"). These records and materials are more specifically identified as:

1. Any and all computer software, including programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs;

2. Any computer-related documentation, which consists of written, recorded, printed or electronically stored material that explains or illustrates how to configure or use computer hardware, software or other related items;

3. Any and all records and materials, in any format and media (including, but not limited to, text messages, SMS messages, picture/video messages, social media communication, envelopes, letters, papers, e-mail, chat logs and electronic messages), pertaining to the Target Offenses;

4. Records and information evidencing occupancy or ownership of the Subject

Device described above, including, but not limited to, sales receipts, registration records, records of payment for Internet access, usernames, passwords, device names, and records of payment for access to newsgroups or other online subscription services;

5. Stored electronic data and related digital storage relating to Global Positioning System ("GPS") data;

6. Records evidencing the use of the Subject Device's capability to access the Internet, including: records of Internet Protocol addresses used and records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

7. Images and videos, to include any metadata identifying the date and location of the Subject Device at the time of the photo or video pertaining to the Target Offenses;

8. Evidence of who used, owned, or controlled the Subject Device at the time the things described in this warrant were possessed, accessed, received, created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

9. Evidence of software that would allow others to control the Subject Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software; and evidence of the lack of such malicious software;

10. Evidence of counter-forensic programs (and associated data) that are designed

to eliminate data from the Subject Device;

11. Evidence of the times the Subject Device was used;

12. Passwords, encryption keys, and other access devices that may be necessary to access the Subject Device.